IN THE CLAIMS:

Amended Claims follow:

1. (Currently Amended) A system for authenticating message data to be exchanged between a sender and a receiver, comprising:

a controller that dynamically selects one of a plurality of authentication mechanisms to be used in providing authentication for an exchange of message data;

a security association and key management module that establishes security associations for said plurality of authentication mechanisms; and

an authentication module that includes support for said plurality of authentication mechanisms, wherein said authentication module generates an authentication tag using an authentication mechanism selected by said control, said authentication tag being appended to said message data;

a1

wherein a portion of a message associated with the message data is processed using a first function that is utilized at least in part to produce the authentication tag;

wherein said portion of said message processed is selected by using a pseudorandom probabilistic function.

2. (Original) The system of claim 1, wherein said controller receives an input identifying a processor load.

3. (Original) The system of claim 1, wherein said controller receives an input identifying an authentication error level.

4. (Original) The system of claim 1, wherein said controller receives an input identifying network defense alarms.

5. (Original) The system of claim 1, wherein said controller receives an input identifying a security policy.

6. (Original) The system of claim 1, wherein said controller includes a network security service resource and one or more security association resource managers contexts, each of said one or more security resource managers contexts being established for a corresponding network application and being responsible for establishing and maintaining an authentication mechanism for a corresponding associated network application, said network security service resource being responsible for providing resource and security constraints within which each of said one or more security resource managers contexts operates.

7. (Original) The system of claim 1, wherein said security association and key management module generates an authentication key for authenticating said message data.

8. (Original) The system of claim 1, wherein said security association and key management module generates a confidentiality key for securing control messages.

9. (Original) The system of claim 1, wherein said security association and key management module operates in accordance with the Internet Key Exchange standard.

10. (Original) The system of claim 1, wherein said authentication module operates in accordance with the IPsec standards.

11. (Currently Amended) A system for authenticating message data to be exchanged between a sender and a receiver, comprising:

a controller that dynamically selects one of a plurality of authentication mechanisms to be used in providing authentication for an exchange of message data; and

an authentication module that generates an authentication tag using said selected authentication mechanism, said authentication tag being appended to said message data;

wherein a portion of a message associated with the message data is processed using a first function that is utilized at least in part to produce the authentication tag;

wherein said portion of said message processed is selected by using a pseudorandom probabilistic function.

12. (Original) The system of claim 1, further comprising a security association and key management module that establishes and maintains said plurality of authentication mechanisms.

13. (Original) The system of claim 2, wherein said security association and key management module operates in accordance with IKE.

14. – 23. (Cancelled)

24. (New) The system of claim 1, wherein said message includes a number of message parts, said message parts are 64-bit words.

25. (New) The system of claim 1, further comprising means for partitioning said message into regions, each region including a number of message parts, and providing one message part from each region as input to said first function.

a1

26. (New) The system of claim 1, wherein said portion of said message processed is selected by:

defining a message selection percentage p; and

using said pseudorandom probabilistic function, uniform over an interval [1, 2L], where L = 1/p and p is a message selection percentage, to determine offsets between message parts which are provided as input to said first function.

27. (New) The system of claim 1, wherein said first function is a keyed hash function.

28. (New) The system of claim 1, wherein said first function is one of an MD4 hashing function, a bucket hashing function, a multilinear modular hashing function, a cyclic redundancy code-based hashing function, and an alternative hash algorithm.

a1

29. (New) The system of claim 1, wherein said portion of said message processed is selected by truncating said message.